September 2, 2021

Dr. Shirley N. Weber, Secretary of State
Office of the Secretary of State
1500 11th St.
Sacramento, California 95814

URGENT: Critical New Risks to the Recall Election Can Be Mitigated by the California Secretary of State

Dear Secretary Weber:

As you know, about three weeks ago, binary images of the Dominion election management system (EMS) were made public. While the software versions are not identical to those used in California, differences are relatively minor: the release materially elevates threats to the trustworthiness of the ongoing California recall election and to public trust in the election. We urge you to address the issue by taking one critical action – a statewide risk-limiting audit (RLA) of trustworthy paper ballots – which can substantially mitigate these threats.

The undersigned are all experts in election cybersecurity. Each of us has well over a decade of continuous experience in that field and a long history of conducting technical studies of voting systems or voting-related cybersecurity, as well as writing, speaking, testifying, making media appearances on many aspects of election integrity. Several of us have served on special panels and task forces appointed by previous California Secretaries of State and have worked closely with local election officials in California.

California has a long history of innovation and national leadership in election security. It was one of the first states to audit elections, with an audit law dating back to the 1960s. It was one of the first states to ban paperless voting systems as a result of a task force appointed by the Secretary of State. The 2007 California Top-To-Bottom Review ("TTBR") was the first state-sponsored review of the security of voting systems and was a huge contribution toward understanding the security issues in all computerized voting systems. Risk-limiting audits (RLAs) were first developed as an outgrowth of a special working group appointed by the Secretary of State, also in 2007, and the first pilot RLAs were conducted in California counties with support from the Secretary of State. California was the second state to have legislation authorizing RLAs and is in the second year of a second set of pilot audits. And California was the first state to expose the dangers inherent in Internet voting, in the report of another Secretary of State's task force in 2000, and was among the first states to ban Internet connections of any kind to its voting equipment. We are thus confident that California election officials are well positioned to take this next step of election security leadership at this critical time.

We are also fully aware of the numerous technical and procedural safeguards California employs to prevent many kinds of administrative errors and to defend against cyber-attacks of various kinds. Many of these were pioneered in California and we acknowledge and applaud them. The security concerns we are writing about here, however, are different from threats we have seen before, and cannot be fully defended against by technical means. The only strong defense against them is the statewide RLA we are recommending for the current election.

The immediate concern

The illegal public release about three weeks ago of binary images of the Dominion election management system (EMS) software and its installation environment constitutes a serious threat to the recall election. Two of the images came from Mesa County, Colorado, and one came from Antrim County, Michigan. Those images, which include the EMS and its installation environment, have been widely downloaded. While it is prudent to assume that other nation states have had that software for a long time, thousands of other people with unknown affiliations, motives, and physical access to voting systems now have it also. That increases the risk of undetected outcome-changing cyber-attacks on California counties that use Dominion equipment and the risk of accusations of fraud and election manipulation which, without rigorous post-election auditing, would be impossible to disprove. While the versions of the Dominion software that were released are not identical to the versions used in California, they are closely related, so this security breach imperils California elections.

Heightened risk of cyber-attack directed against Dominion counties in the recall election

Every complex software system has bugs and security flaws. Cybersecurity research has shown that election software has more than its share. Since that software is usually kept proprietary and secret, however, relatively few people have had the opportunity to examine, instrument, and test it closely enough to find exploitable flaws.

This is now no longer the case, at least with Dominion software. As of August 2021, thousands of unknown people can study the code and find weaknesses to plan attacks on elections. The attacks can be deployed by non-technical accomplices, including voters, building maintenance personnel, and election workers. Unfortunately, even extensive pre-election testing of the voting equipment may not deter or detect such attacks.

The Dominion software from Antrim County has been studied in detail recently by University of Michigan computer science professor Alex Halderman, one of the nation's foremost experts in voting system cybersecurity.[1] While serving as an expert witness in the Curling v. Raffensperger lawsuit in federal court in Georgia, Prof. Halderman found very serious security vulnerabilities in the Dominion Ballot Marking Device (BMD) system, some of which would allow an ordinary voter to insert malware into a BMD during a voting session, with little likelihood of detection. That malware could spread undetected to other voting machines and potentially to the central election management system (EMS) in the county. [2] That EMS software is now in the hands of countless unauthorized people after the Mesa and Antrim releases. Prof. Halderman's full report, dated July 1, 2021, is so sensitive that the Court in Curling v. Raffensperger ordered that it be sealed. We urge you to file a motion with Judge Totenberg to obtain a

[1] Dr. Halderman recently was engaged by Michigan Secretary of State, Jocelyn Benson, to conduct a review of the Antrim County, Michigan Dominion Voting System after human error caused vote count discrepancies in the November 2020 election. (https://www.michigan.gov/documents/sos/Antrim_720623_7.pdf)

[2] Declaration of J. Alex Halderman, 2 August 2021. Curling et al. v Raffensperger et al., United States District Court for the District of Georgia, Northern Division 1:17-cv-2989-AT https://coaltionforgoodgovernance.sharefile.com/d-s7d96b021c2d3419984512b56ff6eee95 (last visited 2 September 2021). In his public declaration Dr. Halderman writes "Attackers could exploit these flaws [in Dominion code] to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. I explain in detail how such malware, once installed, could alter voters' votes while subverting all the procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs). Finally, I describe working proof-of-concept malware that I am prepared to demonstrate in court."

confidential copy of Prof. Halderman's sealed report to inform your cybersecurity team of the vulnerabilities he discovered.

In raising our concerns about the Dominion software release we are not accusing Dominion of wrongdoing. Nor do we have evidence that anyone currently plans to hack the recall election. However, it is critical to recognize that the release of the Dominion software into the wild has increased the risk to the security of California elections to the point that emergency action is warranted.

Emergency measure to secure the election and maintain voter confidence

This newly heightened risk can be mitigated by critical but straightforward action. We urge you to use your authority to mandate a *statewide post-election risk-limiting audit* of the outcome for the two questions on the recall ballot. RLAs have become the widely acknowledged gold standard of post-election auditing. This proposed audit should be done completely transparently, with citizen observation, and under guidance from your office (not vendors or third parties) and under the auspices of local county election officials to maintain Californians' strong voter confidence. RLAs of the outcome require a trustworthy paper trail of hand marked paper ballots with limited use of machine-marked ballots.[3] At least 17 of California's 58 counties—of vastly different sizes and using a broad spectrum of voting systems from different vendors—have already conducted pilot RLAs, so the process is well understood by local election officials. Because the same two contests are on every ballot in the state, a RLA of the recall election is especially straightforward and efficient.

If an actual cyberattack silently changes the outcome of the election, or any other procedural or software error does, a properly conducted RLA based on trustworthy paper ballots will detect it and correct it (with high probability). If the election outcome is correct in the first place the RLA will provide strong public evidence that it is, creating a "firewall" against litigation and disinformation seeking to discredit the outcome.

We believe it is important that a public commitment to such post-election verification be made before Election Day. Otherwise, it may appear to be a partisan decision, and there may be calls for other kinds of "audits" that are neither scientifically grounded nor probative, and that would likely undermine public confidence in the election. We urge you as California's chief election official to take the lead on the auditing issue early and reassure California voters that a thorough transparent audit will promptly follow the election and be completed prior to certifying the results.

We are all willing to discuss any of these points with you or your staff, either in writing or by phone or videoconference or in person in Sacramento. We would be happy to help swiftly design a straightforward, practical, transparent statewide RLA process that will be a model for how high-profile elections should be secured. We would like to be helpful in any way that you find useful to defend against the threats posed

[3] Research shows that voters rarely check machine-printed votes and rarely notice errors when they do check. No audit can determine whether ballot-marking devices printed voters' true selections: if a substantial number of voters use ballot-marking devices, no audit can limit the risk that an incorrect electoral result will be certified. See, e.g., Appel, A., R.A. DeMillo, and P.B. Stark, 2020. Ballot-Marking Devices Cannot Ensure the Will of the Voters, *Election Law Journal: Rules, Politics, and Policy, 19*, https://doi.org/10.1089/elj.2019.0619; Seventh Declaration of Philip B. Stark, 13 September 2020. Curling et al. v Raffensperger et al., United States District Court for the District of Georgia, Northern Division 1:17-cv-2989-AT https://coaltionforgoodgovernance.sharefile.com/share/view/s5ae19303763c45dfa5c8238cb58e47d8 (last visited 2 September 2021); Eighth Declaration of Philip B. Stark, 2 August 2021. Curling et al. v Raffensperger et al., United States District Court for the District of Georgia, Northern Division 1:17-cv-2989-AT https://coaltionforgoodgovernance.sharefile.com/share/view/sbda3c49bc6b646579d6691fb68f2d840 (last visited 2 September 2021)

by the escaped Dominion code and newly discovered Dominion BMD vulnerabilities. Please do not hesitate to call on us to assist. Our contact information is listed with our names below.

Sincerely, and best wishes,

All affiliations below are provided for identification purposes only. The statements and opinions expressed here are not necessarily those of our employers or institutions.

Mustaque Ahamad
Professor, School of Cybersecurity and Privacy, Georgia Tech
mustaq.ahamad@gmail.com

Duncan Buell
NCR Chair in Computer Science and Engineering (Emeritus), University of South Carolina
duncan.buell@gmail.com

Richard A. DeMillo
Charlotte B. and Roger C. Warren Professor of Computer Science and Chair, School of Cybersecurity and Privacy, Georgia Tech
rad@demillo.com

Candice Hoke
Founding Co-Director, Center for Cybersecurity & Privacy Protection, Cleveland-Marshall College of Law, Cleveland State University
shoke@icloud.com

Harri Hursti
Co-founder, Nordic Innovation Labs; Co-founder, Voting Village at DEFCON
harri@hursti.net

David Jefferson
Retired Computer Scientist, Lawrence Livermore National Laboratory
drjefferson@gmail.com

Wenke Lee
John P. Imlay Professor of Computer Science; Director Georgia Tech Cybersecurity Center; School of Cybersecurity and Privacy; Member, Georgia Commission on Safe Secure Elections
wenke.lee@gmail.com

Prof. Philip B. Stark
Professor, Department of Statistics, University of California, Berkeley
pbstark@berkeley.edu